



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/807,824	04/18/2001	Tomoyuki Asano	09812.0501	6164

22852 7590 02/10/2006

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER

JACKSON, JENISE E

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 02/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/807,824	ASANO ET AL.	
	Examiner	Art Unit	
	Jenise E. Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 November 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-114 and 138-161 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-7,20,26-37,56-69,83-95 and 107-114 is/are rejected.
- 7) ☒ Claim(s) 8-19,21-25,38-55,70-82,96-106 and 138-161 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Minor Informalities

1. IDS submitted by Applicant 4/18/2001 cannot be considered by the Applicant until the Applicant provides an English Abstract translation of the documents that are listed on the IDS submitted by the Applicant 4/18/2001. Also, the Applicant is required to submit an English translation of the PCT search report the Applicant submitted on 4/18/2001. The IDS will be considered once the Applicant provides the English translation of the required documents.

Election of Claims by the Applicant

2. A Restriction was made by the Examiner on 10/6/2005. An election was made by the Applicant on 11/3/2005, without traverse to prosecute the invention of Group I, claims 1-114, 138-161. Affirmation of this election was made by the Applicant in writing 11/03/2005. Claims 115-117 and 118-137 are withdrawn from further consideration by the Examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-7, 20, 26-37, 56-69, 83-95, 107-114, are rejected under 35 U.S.C. 102(e) as being anticipated by Harada(6,850,914).

4. As per claims 1, 34, Harada et al. discloses a data transmitting system including a data

Art Unit: 2131

recording medium(i.e. portable medium/ PM)(see col. 4, lines 30-33); and a drive unit which accesses the data recording medium(see col. 5, lines 5-11), the data recording medium including: a security module which executes a mutual authentication protocol with the drive unit and a recording medium proper(see col. 5, lines 5-20, col. 9, lines 26-38); and the drive unit including: a controller which executes the mutual authentication protocol when accessing the data recording medium(see col. 6, lines 35-51); and an interface unit which accesses the recording medium proper of the data recording medium(see col. 7, lines 55-67).

5. As per claim 2, Harada discloses wherein the mutual authentication protocol uses the public-key encryption technology(see col. 9, lines 27-31).

6. As per claim 3, Harada discloses wherein the data recording medium includes the security module and a disc as the data recording medium proper(see col. 8, lines 60-67).

7. As per claim 4, Harada discloses wherein the drive unit further includes means for driving the disc as the recording medium proper of the data recording medium(see col. 8, lines 60-67).

8. As per claim 5, Harada discloses wherein the interface unit accesses directly the recording medium proper(see col. 10, lines 55-59).

9. As per claim 6, Harada discloses wherein the data recording medium includes the security module and a memory chip as the recording medium proper(see col. 5, lines 5-15).

10. As per claim 7, Harada discloses wherein the interface unit accesses the data recording medium via the security module of the data recording medium(see col. 8, lines 60-67).

11. As per claim 26, Harada discloses wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing protocol using the public-key encryption technology, encrypt a data encrypting content key with a shared key thus obtained, and send the encrypted content key

from one of them to the other(see col. 9, lines 1-13, col. 10, lines 43-54).

12. As per claim 27, Harada discloses wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing protocol using the public-key encryption technology, encrypt data with a shared key thus obtained, and send the encrypted data from one of them to the other(see col. 9, lines 1-13, col. 10, lines 43-54).

13. As per claim 35, Harada discloses wherein the mutual authentication protocol is a protocol using the public-key encryption technology(see col. 8, lines 60-67).

14. As per claim 36, Harada discloses wherein the interface unit of the drive unit accesses directly the recording medium proper(see col. 8, lines 35-42).

15. As per claim 37, Harada discloses wherein the interface unit of the drive unit accesses the data recording medium via the security module of the data recording medium(see col. 8, lines 35-50).

16. As per claim 56, Harada discloses wherein when executing the mutual authentication protocol(see col. 8, lines 60-65), the drive unit and security module execute a key sharing protocol using the public-key encryption technology(see col. 8, lines 60-65), encrypt a data encrypting content key with a shared key thus obtained, and send the encrypted content key from one of them to the other(see col. 9, lines 1-20).

17. As per claim 57, Harada discloses wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing protocol using the public-key encryption technology(see col. 8, lines 60-65), encrypt data with a shared key thus obtained, and send the encrypted data from one of them to the other(see col. 9, lines 1-20).

18. As per claim 64, Harada discloses a drive unit, which accesses a data recording medium including a recording medium proper and a security module which executes a mutual authentication protocol with the drive unit(see col. 10, lines 43-59), the drive unit comprising:

a controller which executes the mutual authentication protocol when accessing the data recording medium(see col. 11, lines 26-35); and an interface unit which accesses the recording medium proper of the data recording medium(see col. 11, lines 26-35).

19. As per claim 65, Harada discloses wherein the mutual authentication protocol is a protocol using the public-key encryption technology(see col. 9, lines 26-30).

20. As per claim 66, Harada discloses further comprising a drive means for driving a disc as the recording medium proper of the data recording medium(see col. 8, lines 60-67).

21. As per claim 67, Harada discloses wherein the interface unit accesses a memory chip as the recording medium proper of the recording medium(see col. 5, lines 5-15).

22. As per claim 68, Harada discloses wherein the interface unit accesses directly the recording medium proper(see col. 8, lines 60-67).

23. As per claim 69, wherein the interface unit accesses the recording medium proper of the data recording medium via the security module of the data recording medium(see col. 8, lines 60-67, col. 9, lines 1-13).

24. As per claim 83, Harada discloses adapted to work with the security module, when executing the mutual authentication protocol, in executing a key sharing protocol using the public-key encryption technology(see col. 8, lines 60-67), encrypt a data encrypting content key with a shared key thus obtained, and send the encrypted content key from one of the drive unit and security module to the other(see col. 9, lines 1-13).

25. As per claim 84, Harada discloses adapted to work with the security module, when executing the mutual authentication protocol, in executing a key sharing protocol using the public-key encryption technology(see col. 8, lines 60-67), encrypt data with a shared key thus obtained, and send the encrypted data from one of the drive unit and security module to the other(see col. 9, lines 1-13).

Art Unit: 2131

26. As per claims 28-33, 58-63, 85-90, 109-114, Harada discloses destined to write data to the recording medium proper via the interface unit, wherein: a protocol for key sharing with the security module is executed using the public-key encryption technology the data content key is encrypted with the shared key obtained through the execution of the key sharing protocol(see col. 9, lines 39-44) and the encrypted data content key is sent to the security module; the security module decrypts the encrypted content key with the shared key obtained through the execution of the key sharing protocol(see col. 9, lines 39-47), and receives data re-encrypted with the content key decrypted with save key stored therein; and the data encrypted with the content key and the content key encrypted by the security module using the save key are recorded to the recording medium proper via the interface unit(see col. 10, lines 55-67, col. 11, lines 1-7).

27. As per claim 91, Harada discloses access method for access to a data recording medium including a recording medium proper and a security module which executes a mutual authentication protocol with a drive unit(see col. 9, lines 27-38), the method comprising steps of: executing the mutual authentication protocol when accessing the data recording medium; and accessing the recording medium proper of the data recording medium according to the result of the mutual authentication protocol execution(see col. 10, lines 31-65).

28. As per claim 92, Harada discloses wherein the mutual authentication protocol is a protocol using the public-key encryption technology(see col. 9, lines 27-38).

29. As per claim 93, Harada discloses where access is made to a memory chip as the recording medium proper of the data recording medium(see col. 5, lines 5-15).

30. As per claim 94, Harada discloses wherein access is made directly to the recording medium proper(see col. 8, lines 60-67).

31. As per claim 95, Harada discloses wherein the interface unit accesses the

Art Unit: 2131

data recording medium via the security module of the data recording medium(see col. 8, lines 60-67, col. 9, lines 1-13).

32. As per claim 107, Harada discloses wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing protocol using the public-key encryption technology(see col. 10, lines 43-59), encrypt, using a shared key thus obtained, a data encrypting content key, and send the encrypted content key from one of them to the other(see col. 11, lines 26-35).

33. As per claim 108, Harada discloses wherein when executing the mutual authentication protocol, the drive unit and security module execute a key sharing protocol using the public key encryption technology(see col. 9, lines 27-37, col. 10, lines 43-65), encrypt data with a shared key thus obtained, and send the encrypted data from one of them to the other(see col. 10, lines 49-55).

34. Claims 8-19, 21-25, 38-55, 70-82, 96-106, 138-161 are objected to as being rejected on base claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

• Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



February 4, 2006


2/6/06